AMENDMENTS TO THE SPECIFICATION

Please amend original paragraph [0003] as reflected in the following, marked-up version of the paragraph:

[0003]   Web-servers as well as user computers have various security concerns and the exchange of information between a user computer and a web site is one ~~or~~ of the reasons that security is required to protect the information.   One of the more common security concerns is cross-site scripting.   Cross-site scripting attacks typically occur in scenarios where a server generates a dynamic web page.   By creating a dynamic web page, the server may relinquish control over how the output is interpreted by the user computer.   In a cross-site scripting attack, a security issue arises if untrusted dynamic content can be introduced into a dynamic page.

Please amend original paragraph [0005] as reflected in the following, marked-up version of the paragraph:

[0005]   On the Internet, many web-servers are unknowingly vulnerable to cross-site scripting attacks.   Even though cross-site scripting attacks can be practically eliminated by rigorously validating and encoding data, many developers do not have the experience or knowledge to do this effectively.   In addition, an approach that encodes all output has an impact on performance and may destroy data by encoding previously encoded data.   There is a need for systems and methods that ~~mitigating~~ mitigate cross-site scripting attacks.

Please amend original paragraph [0021] as reflected in the following, marked-up version of the paragraph:

[0021]   Cross site scripting attacks can be prevented or mitigated by examining the HTTP request for active content.   Active content includes, by way of example and not limitation, scripts, expressions, events, object tags, and the like.   The HTTP request is examined by searching for markers such as script constructs or other markers of active content.

Page 2 of 14

Please amend original paragraph **[0024]** as reflected in the following, marked-up version of the paragraph:

[0024]   When a request is received, the request is search<u>ed</u> for markers of active content. A server computer, for example, may maintain a list of markers of active content. The markers of active content in the list can be updated as needed or augmented with additional markers of active content. Existing markers of active content can also be deleted or made inactive. In other words, the ability of a server to recognize a cross-site scripting attack can be enhanced over time by refining the list.

Please amend original paragraph **[0028]** as reflected in the following, marked-up version of the paragraph:

[0028]   For example, a query string ~~300~~ 302 may have the form NAME1=VAL1 & NAME2 = VAL2. The user input in this example is data at risk for the injection of a script. The data at risk in this example is "VAL1" and "VAL2." The server computer may only examine the data at risk for script constructs in one embodiment. In such an embodiment, for example, in a query string, the server computer may only need to examine the data provided by the user.

Page 3 of 14